Method of defense-in-depth ultrasound intrusion detection.
Inventors: Robert H. Roche, et al. Application No: 10/754,800. New Sheet.

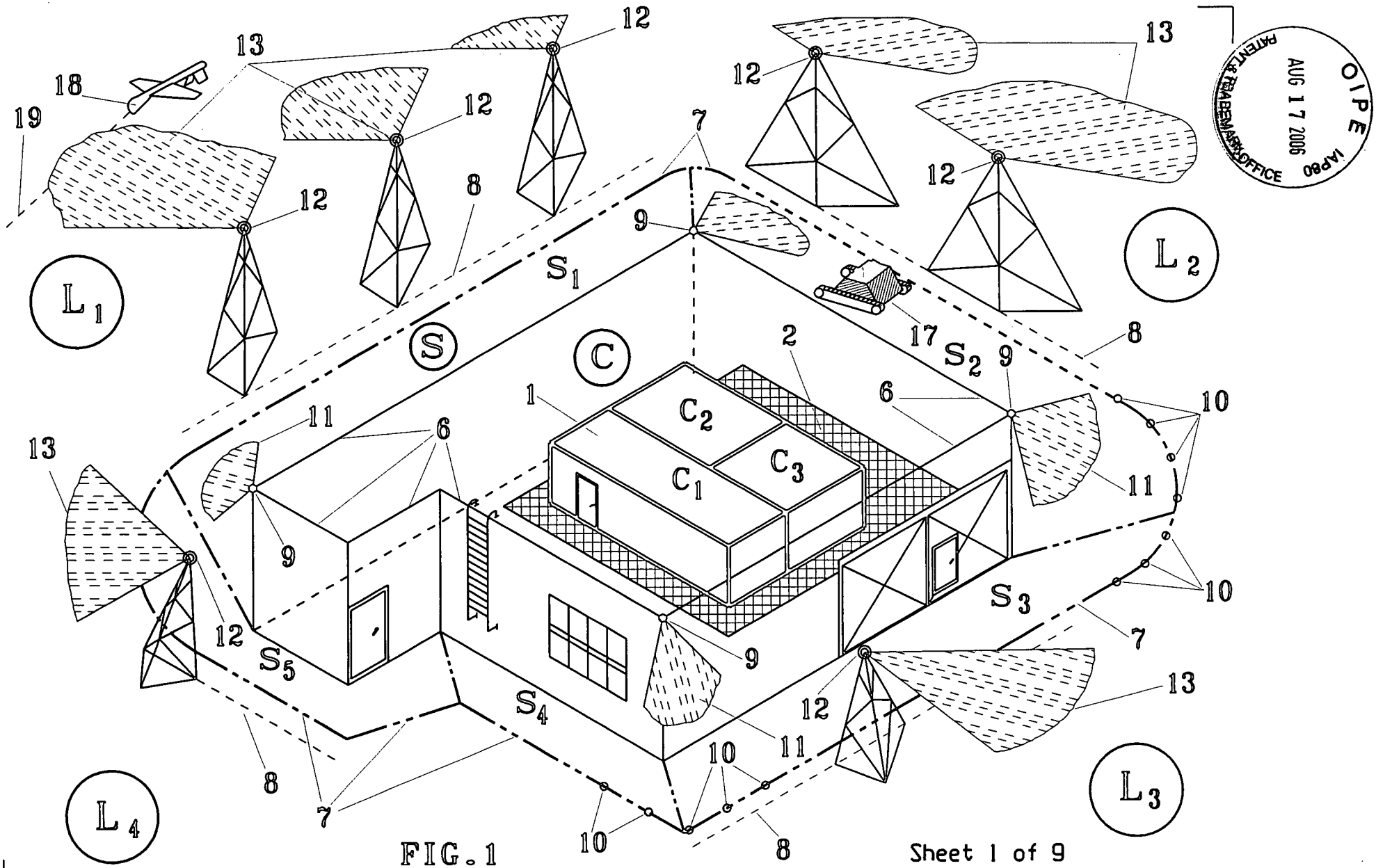
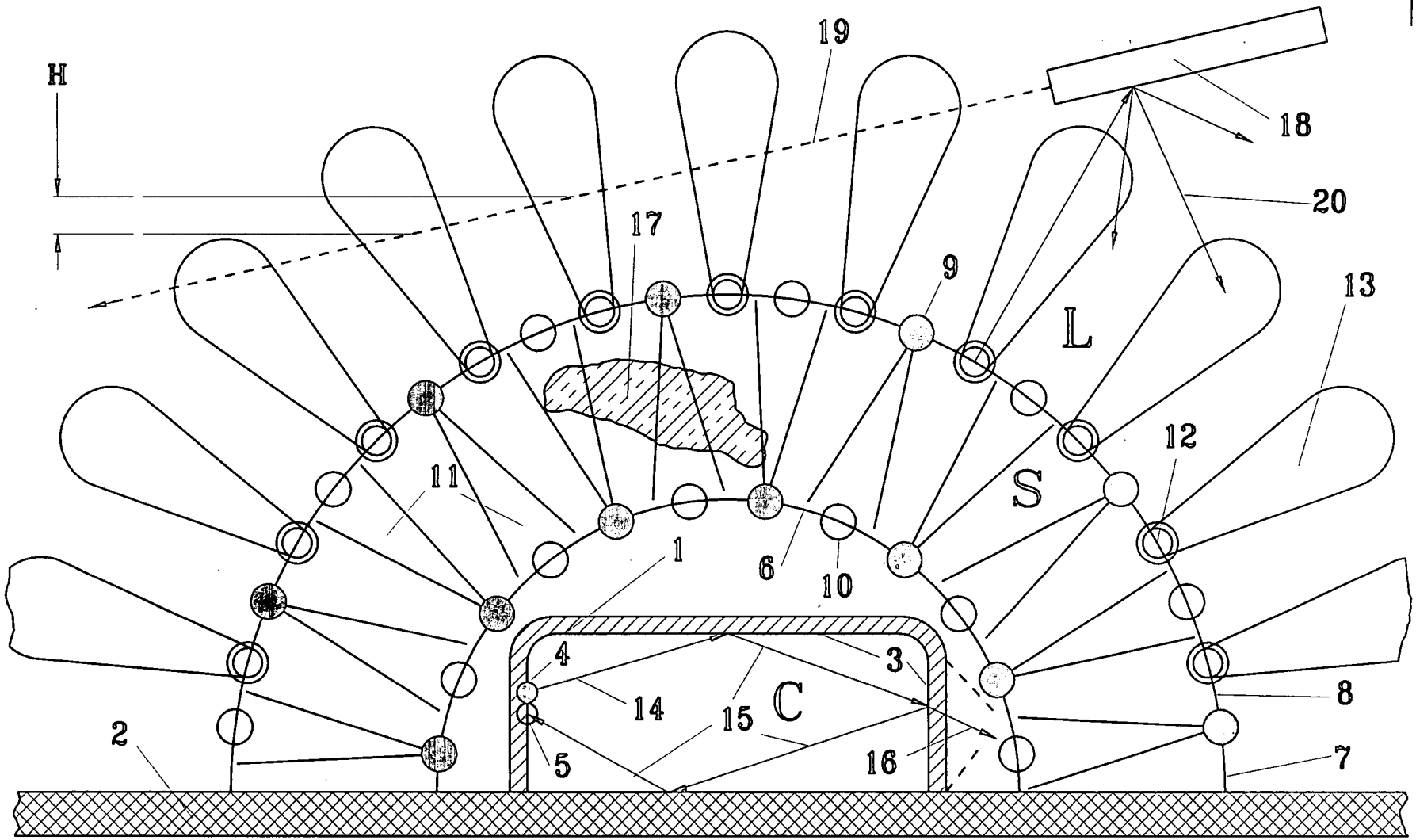


FIG. 1



◎ - Transmitters/Receivers of Long -Range Echelon

○ - Receivers of Central and Short-Range Echelons

⊙ - Transmitters of Central and Short-Range Echelons

FIG. 2

Alternative sequences of detected signals in echelons			Versions of intrusion in eshelons			Versions of self-checking results	Notes
C	S	L	Ingress	Egress	Presence inside		
C ⟶ C					+	May also mean an unauthorized discloser of protected housing.	Emitted ultrasound goes outside.
C ⟶ S				+		Target moves to echelon L ? Check it.	
S ⟶ C			+			Target moves from echelon L ? Check it. Echelon L may be in the failed state.	
C ⟶ L				+		Target moves inside echelon L ? Check it. Echelon S may be in the failed state.	
L ⟶ C			+			Target moves inside echelon C ? Check it. Echelon S may be in the failed state.	
	S ⟶ S				+	Target moves in echelon S? Check it. Other echelons C and L may be in the failed state.	
	S ⟶ L			+		Target moves from echelon C ? Check it. Echelon C may be in the failed state.	
	L ⟶ S		+			Target moves to echelon C? Check it. Echelon C may be in the failed state.	
		L ⟶ L			+	Target moves inside echelon L ? Check it. An intruder may not be threat if it passes by the echelon S.	

Note: Arrows show the directional sequence of caution signals from intrusion-suspected echelons.

FIG. 3

Sublevels of echelons (in indices of FIG.3)	L_1	L_2	L_3	L_4	S_1	S_2	S_3	S_4	S_5	C_1	C_2	C_3	**Expected sequent events and real menaces at single intrusion**
L_1	X												VAM, PO, OCF, CCF.
L_2		X											VAM, PO, OCF, CCF.
L_3			X										VAM, PO, OCF, CCF.
L_4				X					X				VAM, PO, OCF, CCF.
S_1					X					X			VAM, OCF.
S_2	X					X							VAM, IF.
S_3					X		X					X	VAM, LF.
S_4				X				X					VAM, CCF.
S_5		X				X			X				VAM, CCF.
C_1	X		X		X		X	X		X	X		VAM, SSF.
C_2											X		VAM, CCF.
C_3							X					X	VAM, SSF, CCF.
Expected sequent events and real menaces at multiple intrusion	CCF	CCF	PO, DF	PO, DF	IF, DF	DF	DF, SSF	SSF CCF	LF, SCF	LF, DF	CCF	DF, PO	*The pre-designed samples of vulnerability of surveyed areas are being kept in archive data file.*

FIG. 4

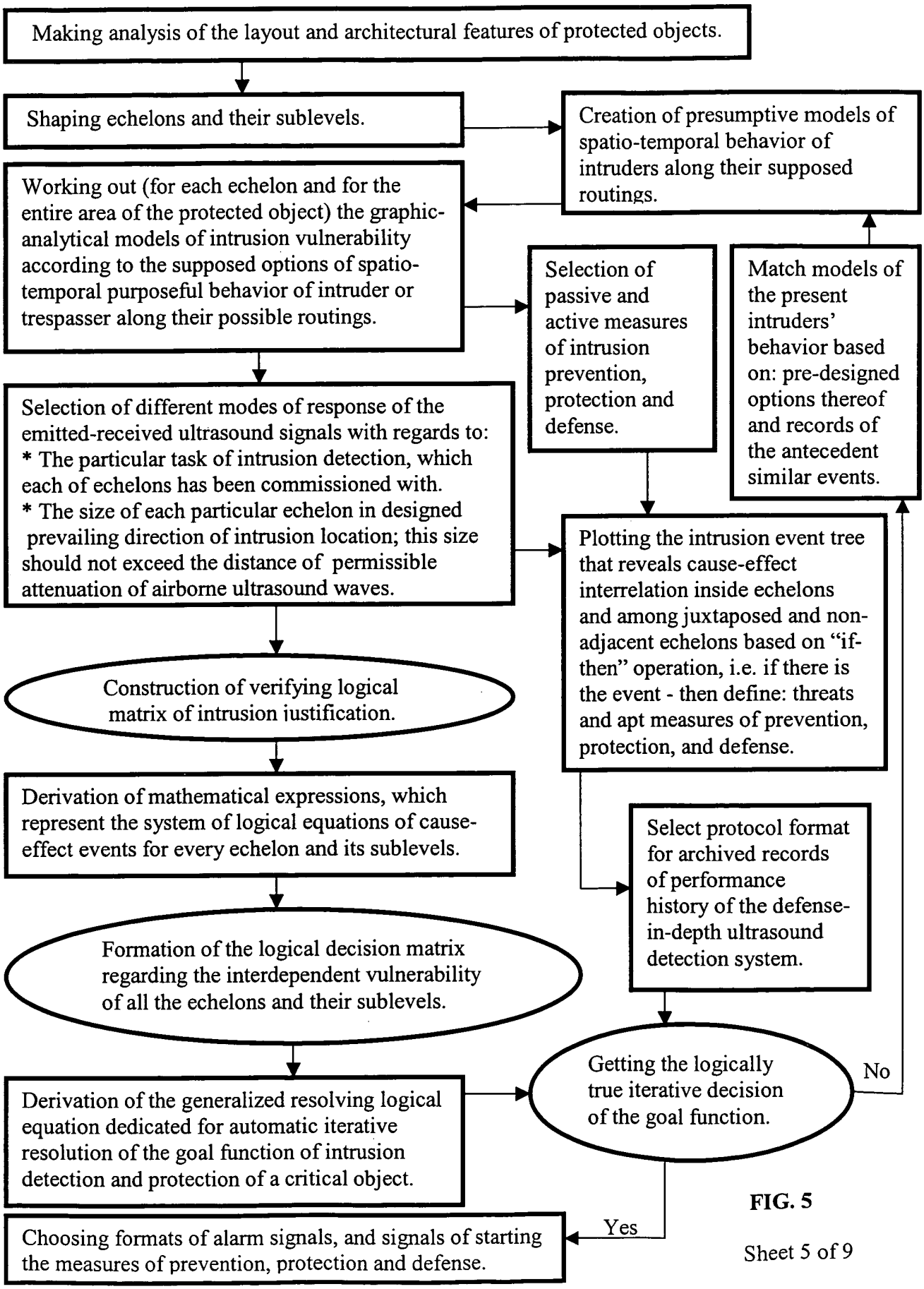

Making analysis of the layout and architectural features of protected objects.
Shaping echelons and their sublevels.
Creation of presumptive models of spatio-temporal behavior of intruders along their supposed routings.
Working out (for each echelon and for the entire area of the protected object) the graphic-analytical models of intrusion vulnerability according to the supposed options of spatio-temporal purposeful behavior of intruder or trespasser along their possible routings.
Selection of passive and active measures of intrusion prevention, protection and defense.
Match models of the present intruders' behavior based on: pre-designed options thereof and records of the antecedent similar events.
Selection of different modes of response of the emitted-received ultrasound signals with regards to:
* The particular task of intrusion detection, which each of echelons has been commissioned with.
* The size of each particular echelon in designed prevailing direction of intrusion location; this size should not exceed the distance of permissible attenuation of airborne ultrasound waves.
Plotting the intrusion event tree that reveals cause-effect interrelation inside echelons and among juxtaposed and non-adjacent echelons based on "if-then" operation, i.e. if there is the event - then define: threats and apt measures of prevention, protection, and defense.
Construction of verifying logical matrix of intrusion iustification.
Derivation of mathematical expressions, which represent the system of logical equations of cause-effect events for every echelon and its sublevels.
Select protocol format for archived records of performance history of the defense-in-depth ultrasound detection system.
Formation of the logical decision matrix regarding the interdependent vulnerability of all the echelons and their sublevels.
Getting the logically true iterative decision of the goal function.
No
Derivation of the generalized resolving logical equation dedicated for automatic iterative resolution of the goal function of intrusion detection and protection of a critical object.
Yes
Choosing formats of alarm signals, and signals of starting the measures of prevention, protection and defense.

FIG. 5

Data Files of Operative Algorithm	Stages of System's Design and Operation	Data Record and Input Format	Data Processing Formats and Modes	Note
Predetermined Design Data	Design of multi-echelon arrangement of ultrasound detection system. Definition of its adjustment and starting-up basics.	Models of echelons' and entire protected area's intrusion vulnerability based on the presumptive models of intruders' run.	Optional spatio-temporal routings of intruders with cause-effect evaluation of vulnerability of facilities and the whole of object.	The size of each echelon is being rated in accordance with airborne ultrasound wave attenuation along its incidence-reflection trip.
Data batch entry under commissioning: Data batch entry during operation:	Evaluation of cause-effect intrusion menaces and potential vulnerabilities. Plotting spatio-temporal data of intrusion routings.	Intrusion event tree that represents cause-effect interdependent menaces among echelons. Analysis of modeled and running intrusion data.	The event tree in tabular or flow-chart format based on the "if-then" operation. Look-up table of modeled previously and current data of intrusion menaces.	The properly selected modes of response of emitted ultrasound signals predict the sequent correct determination of cause-effect intrusion events.
Informational and Processing Inter-echelon Interrelation	Vindication of single or group intrusion detection signals. Accomplishment of final, logically true decision of goal function of intrusion detection and protection.	Entry of caution and self-checking signals into verifying logical matrix. Iterative resolution of the goal function during continuous status scan and data acquisition.	Entry of resulted data of treatment of caution and self-checking signals into: local logical equations of echelons, logical decision matrix and generalized resolving logical equation.	The current operation of system's data control block provides for data acquisition (in particular: caution and self-checking signals) due to continuous status scan of all detectors.
Intermediate derived data: Finalized derived data:	The decisions of: logical equation of each echelon; logical decision matrix. The decision of generalized resolving logical equation.	The menaces of echelons and their sublevels, and entire threat to the object. The resolution of goal function of protection.	Data of continuous status scan input into any logical equation and into logical decision matrix only thru verifying logical matrix.	The verifying logical matrix analyses all caution and self-checking signals to avoid fault resolutions of the goal function.
Executive and Actual Instructions	Generation and entry of alarm signals and signals for actuation measures of prevention, protection and defense.	Entry of instructions for: Start of local preventive measures; and Carrying out passive and active measures of final protection and defense.	Preferably the preventive local measures include entry of warning signals, actuation of barriers and entrapments against an intruding subject.	Alarm signals are being represented in the result of justification of caution signals for really effected echelon by the verifying logical matrix.
Trip and Results Log	Sampling and archiving the historical files of safety and security maintenance.	Continuous archiving all the samples of operating status of the system.	Informational archive data transferring goes in the two-way exchange mode.	Use from archive data file the antecedent resolutions of the goal function.

FIG. 6

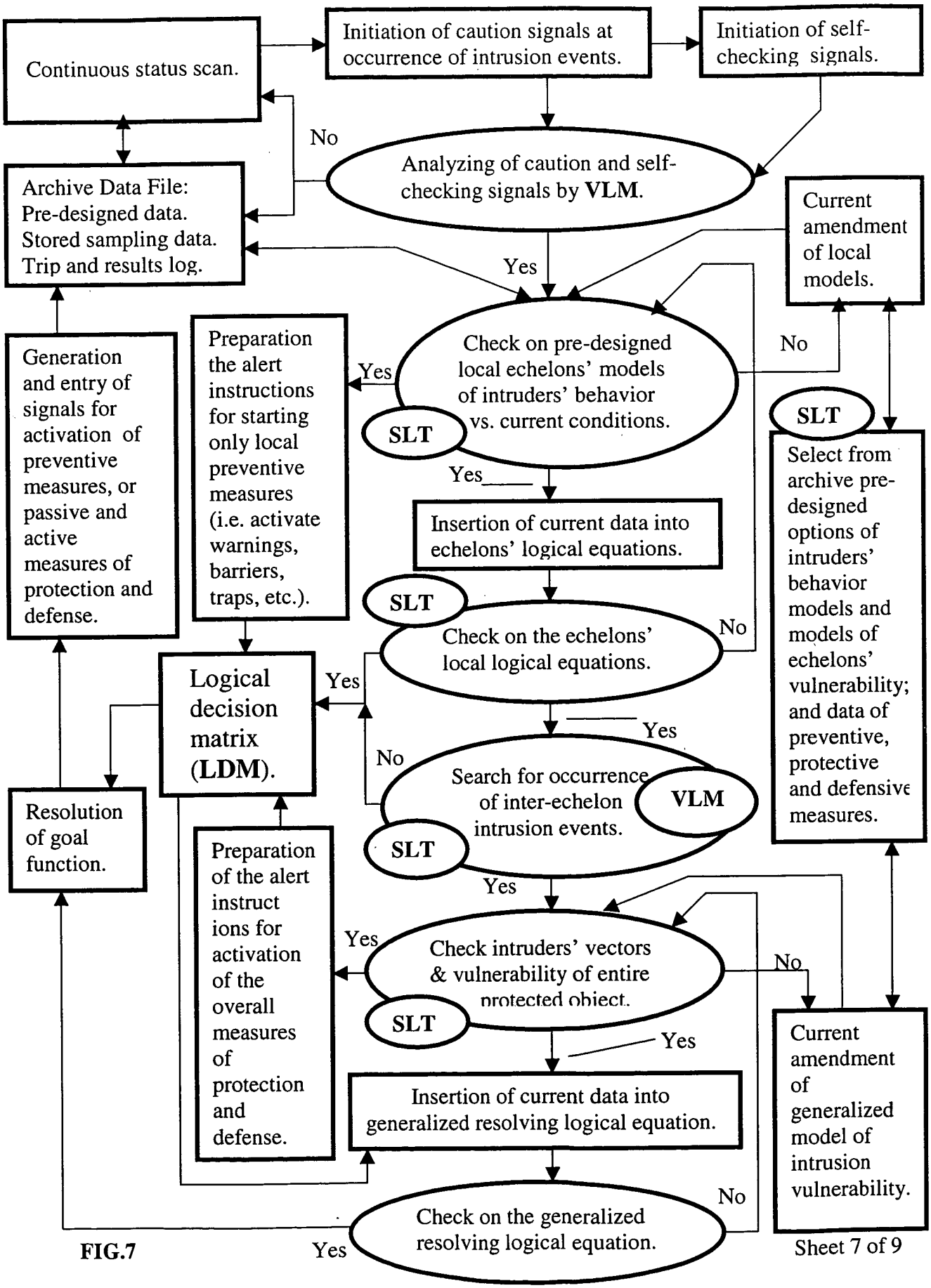

Continuous status scan.
Initiation of caution signals at occurrence of intrusion events.
Initiation of self-checking signals.
No
Analyzing of caution and self-checking signals by VLM.
Archive Data File:
Pre-designed data.
Stored sampling data.
Trip and results log.
Current amendment of local models.
Yes
Generation and entry of signals for activation of preventive measures, or passive and active measures of protection and defense.
Preparation the alert instructions for starting only local preventive measures (i.e. activate warnings, barriers, traps, etc.).
Yes
Check on pre-designed local echelons' models of intruders' behavior vs. current conditions.
SLT
No
SLT
Select from archive pre-designed options of intruders' behavior models and models of echelons' vulnerability; and data of preventive, protective and defensive measures.
Yes
Insertion of current data into echelons' logical equations.
SLT
Check on the echelons' local logical equations.
No
Logical decision matrix (LDM).
Yes
Yes
No
Search for occurrence of inter-echelon intrusion events.
VLM
SLT
Resolution of goal function.
Preparation of the alert instruct ions for activation of the overall measures of protection and defense.
Yes
Yes
Check intruders' vectors & vulnerability of entire protected object.
No
SLT
Yes
Insertion of current data into generalized resolving logical equation.
Current amendment of generalized model of intrusion vulnerability.
No
Check on the generalized resolving logical equation.
Yes

FIG.7

Indices of echelons and sublevels therein	Event occurrence logical equation	Factors of menaces in the order of diminishing rate	Pre-designed selective security measures
L_1	$L_1 + (L_1 \cdot S_2) + (L_1 \cdot C_1)$ = High level threat (**HT**)	(PO+OCF+CCF) • VAM	VAM + PO, →Intrusion prevention and start backup power. Other menaces, → Measures of intrusion protection and defense.
L_2	$L_2 + (L_2 \cdot S_5)$ = High level threat (**HT**)	(CCF + OCF + PO) • VAM	The same as for L_1.
L_3	$L_3 + (L_3 \cdot C_1)$ = Low level threat (**LT**)	(PO + DP) • VAM	Intrusion prevention : activate backup power, warnings, barriers, etc.
L_4	$L_4 + (L_4 \cdot S_4)$ = **LT**	(PO + DP) • VAM	Intrusion prevention : activate backup power, warnings, barriers, etc.
L	$(L_1+L_2+L_3+L_4) + (L_1 \cdot L_2 \cdot L_3 \cdot L_4)$ = **HT**	(CCF+PO+OCF) • VAM	Selective activation of intrusion prevention, protection and defense.
S_1	$S_1 + (S_1 \cdot S_3) + (S_1 \cdot C_1)$ = **LT**	(DF + IF) • VAM	Intrusion prevention : activate barriers, traps, redundant blocks, etc.
S_2	$S_2 + (S_2 \cdot S_5)$ = **LT**	DF • VAM	Intrusion prevention : activate barriers, traps, redundant blocks, etc.
S_3	$S_3 + (S_3 \cdot C_1) + (S_3 \cdot C_3)$ = Moderate level threat (**MT**)	(SSF + DF) • VAM	Selective activation of intrusion prevention, protection and defense.
S_4	$S_4 + (S_4 \cdot C_1)$ = **HT**	(CCF + SSF) • VAM	Passive and active measures of intrusion protection and defense.
S_5	$S_5 + (S_5 \cdot L_4)$ = **MT**	[(LF + SCF) • VAM] + [(LF • SCF) • VAM]	Selective activation of intrusion prevention, protection and defense.
S	$(S_1+S_2+S_3+S_4+ S_5) + (S_1 \cdot S_2 \cdot S_3 \cdot S_4 \cdot S_5)$ = **HT**	{[CCF + (SSF + DF + LF + SCF +IF)] + [(SCF • LF) + (SSF • DF) + SCF]} •VAM	Selective activation of intrusion prevention, protection and defense.
C_1	$C_1 + (C_1 \cdot S_1)$ = **MT**	{[SSF • (LF + DF)] +[(SSF • LF • DF)]} • VAM	Selective activation of intrusion prevention, protection and defense.
C_2	$C_2 + (C_2 \cdot C_1)$ = **HT**	CCF • VAM	Passive and active measures of intrusion protection and defense.
C_3	$C_3 + (C_3 \cdot S_3)$ = **HT**	[CCF + (CCF • SSF) + (CCF • DF) + (CCF •PO) + (SSF • DF) + (SSF • PO)] • VAM	Passive and active measures of intrusion protection and defense.
C	$(C_1+C_2+C_3) + (C_1 \cdot C_2 \cdot C_3)$ = **HT**	{CCF +[(CCF • SSF) + (SSF • DF) + (LF • DF)] • PO} • VAM	Selective activation of intrusion prevention, protection and defense.
GRLE	[(L • S) + (S • C) + (L • S • C)] + [(L • C) + (C • S) + (C • S • L)] = **HT**	{[(CCF + (CCF • SSF) + (LF • OCF) + (SSF • SCF) + (SSF • DF • IF)] • PO} • VAM	Passive and active measures of intrusion protection and defense.

FIG.8

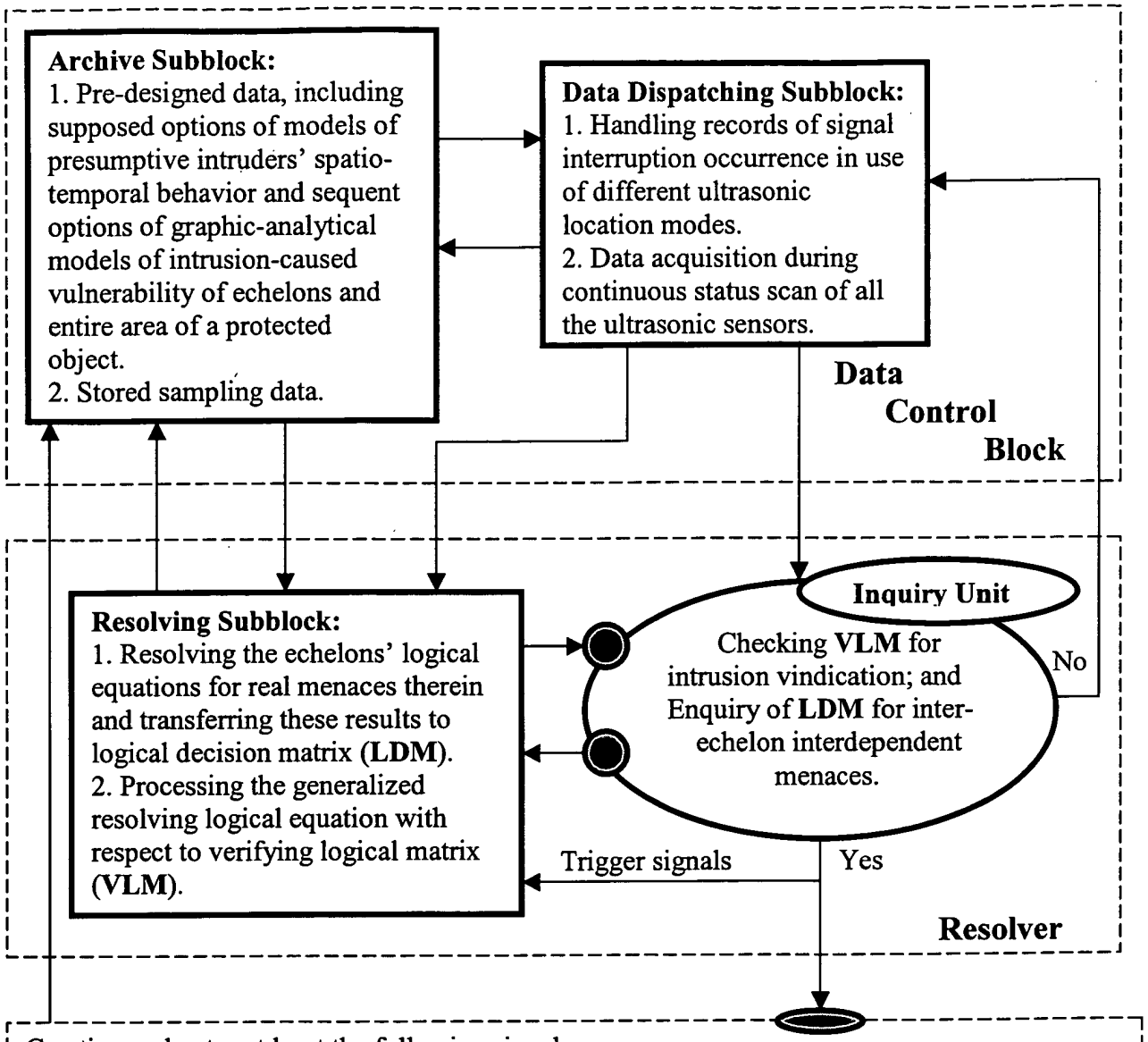

Archive Subblock:
1. Pre-designed data, including supposed options of models of presumptive intruders' spatio-temporal behavior and sequent options of graphic-analytical models of intrusion-caused vulnerability of echelons and entire area of a protected object.
2. Stored sampling data.
Data Dispatching Subblock:
1. Handling records of signal interruption occurrence in use of different ultrasonic location modes.
2. Data acquisition during continuous status scan of all the ultrasonic sensors.
Data Control Block
Resolving Subblock:
1. Resolving the echelons' logical equations for real menaces therein and transferring these results to logical decision matrix (LDM).
2. Processing the generalized resolving logical equation with respect to verifying logical matrix (VLM).
Inquiry Unit
Checking VLM for intrusion vindication; and Enquiry of LDM for inter-echelon interdependent menaces.
No
Yes
Trigger signals
Resolver
Creation and entry at least the following signals:
1. The caution signals as the primary signs of intrusion detection.
2. The self-checking signals as the direct evidence of sense wires' integrity, and as the indirect justification of intrusion detection.
3. The alarm signal as the evidence of intrusion vindication for the really effected echelon, where the entry of that signal is the result of analysis of caution and self-checking signals done by verifying logical matrix (VLM).
4. The signal for activation the intrusion preventive measures, i.e. closing physical barriers (gates, doors, hatches, etc.) for isolation of an intruding subject (unmanned ground vehicle, mini-robot, etc.), or a trespasser.
5. The signal for activation passive and active measures of protection and defense, which signals are being created in the result of the logically correct decision of the goal function of this intrusion detection and protection method.
System Control Block

FIG.9